DENIM GROUP **APPENDIX F TO DIR CONTRACT NO. DIR-SDD-1850**

## SAMPLE SOW DOCUMENT

| | |
|---|---|
| **Prepared For:** | **CUSTOMER** |
| **Document Title:** | **Statement of Work – XXX Application Black Box Security Assessment** |
| **Doc Issue Date:** | DATE |
| **Doc Expiry Date:** | 30 days from issue date |
| **Doc File Name:** | _XXXAppBBSecAssess_SOW_v1 |
| **Doc Status:** | Ver 1.0 for sign off by Customer POC |
| **Author:** | Aaron Copeland, aaron@denimgroup.com, (210) 572-4400 |
| **Customer Contact:** | **CUSTOMERPOC** |
| **Title:** | TITLE |

## Introduction

Customer () would like Denim Group to provide an enhanced black box assessment to analyze the security state of its XXX application. Denim Group will assess the security of the application by simulating the activities of an external attacker. As such, Denim Group will use a variety tools and approaches to characterize how the application responds to both automated and manual attacks from outside the trusted network. Although the assessment will commence with automated scans of the application to characterize the attack surface of the system, there will be an emphasis throughout the project on manual enumeration of the XXX Application. These manual tests will attempt to identify flaws in application logic and trust boundary violations within the XXX system.

This black box security engagement will include a final written report as well as an on-site technical debrief. Denim Group's final written deliverable will include an executive summary, vulnerability observations, and proposed remediation recommendations to address the security state of the application. Denim Group will propose remediation strategies in order to enable to develop a remediation plan to address vulnerabilities observed during the assessment.

## Statement of Work

Denim Group will provide a black box security assessment of the XXX application in order to observe application vulnerabilities and flaws that could be exploited by an outside attacker as well as activities from perspective of a credentialed insider.

The assessment of the XXX application will include automated and manual tests of the application from an external viewpoint (i.e. black box), as well as tests to determine whether authorized users can elevate access and privileges. Denim Group's assessment methodology is based on the emerging industry standard defined by the Open Web Application Security Project (OWASP) which captures the major classes of web application vulnerabilities that might exist in the XXX application. Once identified, vulnerabilities are assigned a classification and rating which clarifies their respective type and severity for remediation.

Denim Group's deliverables will include a risk ranking, explanation of findings, and suggested remediation strategies to address vulnerabilities in the system. The deliverable will also identify the findings in the expanded test coverage (manual testing), above and beyond the scope of traditional automated application scanning in effort to provide with key insight into existing vulnerabilities as well as strategies that will help enable to remediate flaws observed during the assessment. The end deliverable's remediation recommendations will also be tailored to meet the overall objectives of organizational application security remediation plan and will address strategies for the execution of secure application development remediation.

## Scope of Work

The scope of work is defined as follows:

| **Black Box** | | | **Action** | **Deliverables** |
|---|---|---|---|---|
| | | | | |
| | 1 | Kick off meeting | Conference Call with | |
| | 2 | Meet with application experts | Conference Call with | |
| | 3 | Discovery and enumeration with automated tools, such as the WatchFire AppScan scanning tool | | |
| **Milestone** | 4 | Manual characterization of vulnerabilities and penetration testing | | |
| **Milestone** | 5 | Compile report for black box security assessment | | **D1** Observations and Recommended Remediation Report |
| **Milestone** | 6 | Black Box Security Assessment completion review | Meeting or Conference call with | **D2** PowerPoint presentation of Observations and Recommended Remediation |

## Deliverables

The deliverables are defined in detail as follows:

| **Deliverable** | **Description** |
|---|---|
| **D1** Observations and Recommended Remediation Report | The final report will include observations from the application security assessments. Recommendations for remediation will be made in the form of various examples. These recommendations will include examples of insecure and more secure coding idioms, as they relate to the assessed applications, as well as examples of insecure and more secure design and architecture procedures. The report will identify problematic coding trends, provide in-depth vulnerabilities reporting, as well as remediation recommendations of the application. |
| **D2** Application Security Assessment Completion Review | The Completion Review is a PowerPoint presentation of assessment activities, observations/findings, and recommendations on-site with key application specific m members. |

| | |
|---|---|

## SAMPLE SOW DOCUMENT

## Assumptions

1. The majority of testing will be conducted from Denim Group offices over the Internet or a mutually agreeable VPN technology.
2. application experts will be made available to meet with Denim Group consultants as required.
3. All testing will be performed on systems in a non-production (i.e. staging) environment to minimize or eliminate any chance that production systems or production data will be affected by testing. will provide the system (hardware, software, installation, and configuration) to Denim Group prior to the start of the engagement. For the purposes of this evaluation, the state of the testing system (i.e. operating system and network configuration) will be assumed to be equivalent to the production systems.
4. Testing will be performed from the Denim Group offices during business hours.
5. will provide Denim Group with all necessary access to the application and necessary environments during the engagement.

## Timeline

A project plan and timeline will be formulated following the kickoff meeting. Access and application availability will impact the project timeline.

## Terms

**Price:** Project is fixed at $________
**Payments:** To be made in accordance with Section 6.C of Appendix A to DIR Contract No. DIR-SDD-1850 and upon the following milestones:

| Milestone | Payment |
|---|---|
| 1. Upon completion of Black Box assessment activities | $ |
| 2. Delivery of the Observations and Recommended Remediation Report | $ |
| 3. Delivery of Black Box Security Assessment Completion Review | $ |

Work beyond the scope defined in this statement of work will be handled under a “change order” statement of work.

Denim Group anticipates some travel and expenses related to this project. Expenses and materials are charged at cost. All travel, expenses and materials will be approved by prior to being incurred or acquired and receipts can be provided.

Denim Group will perform the items under this Statement of Work during the course of normal business hours, 8am to 6pm CST Monday through Friday. Any scheduling required by outside of this timeframe is subject to an “after-hours” rate change of $______ per hour.

Customer may cancel this project by relinquishing the deposit, or by paying for the amount of work done at the time of cancellation at the rate of $_____ per hour, whichever is larger.

## Start Date

## SAMPLE SOW DOCUMENT

Start date depends on signed statement of work and availability of resources.

## DOCUMENT SIGN OFF

| | |
|---|---|
| **Fax To:** | **Allyn McClendon, allyn@denimgroup.com, (210) 572-4400** |
| | **Operations Coordinator** |
| | **Denim Group** |
| **DGFax #** | **(210) 572-4401** |

| | |
|---|---|
| **Prepared For:** | **Customer** |
| **Document Title:** | **Statement of Work – XXX Application Black Box Security Assessment** |
| **Doc Issue Date:** | DATE |
| **Doc Expiry Date:** | 30 days from issue date |
| **Doc File Name:** | XXXAppBBSecAssess_SOW_v1 |
| **Doc Status:** | Ver 1.0 for sign off by CUSTOMER POC |
| **Author:** | Aaron Copeland, aaron@denimgroup.com, (210) 572-4400 |
| **Customer Contact:** | Customer POC |
| **Title:** | TITLE |

| **Signature** | **Signature denotes acceptance of above listed document contents and approval to proceed.** |
|---|---|
| **Signature:** | |
| **Name:** | |
| **Title:** | |
| **Date:** | |

| **Denim Group Signature** | **Signature denotes acceptance of above listed document contents and intent to proceed.** |
|---|---|
| **Signature:** | |
| **Name:** | |
| **Title:** | |
| **Date:** | |